UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

SHIRA HAID, individually and on behalf of all others similarly situated, Plaintiff, v. ONETOUCHPOINT CORP., Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Shira Haid ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendant OneTouchPoint Corp. ("OTP") and complains and alleges upon personal knowledge as to herself and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against OTP for its failure to secure and safeguard her and approximately 1,073,316 other individuals' personally identifiable information ("PII") and personal health information ("PHI"), including names, addresses, healthcare member IDs, and other information provided during health assessments.

2. Defendant is a mailing and printing services vendor, which offers print, marketing execution, and supply chain management services to organizations in the healthcare sector.

3. On or around April 28, 2022, OTP detected encrypted files on some of its systems and began investigating the incident.

4. OTP's investigation later revealed that an unauthorized party had accessed certain OTP servers on April 27, 2022 (the "Data Breach").

5. On or around June 3, 2022, OTP provided a summary of its investigation to its customers. It did not send out letters to individuals impacted by the breach until July 27, 2022.

6. OTP reported that the scope of information involved includes an individual's name, member ID, and information that may have been provided during a health assessment, including dates of service, description of service, diagnosis codes, and other medical information.

7. OTP owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class members' PII/PHI against unauthorized access and disclosure. OTP breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect patients' PII/PHI from unauthorized access and disclosure.

8. As a result of OTP's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and individuals in the United States whose PII/PHI was exposed as a result of the Data Breach, which OTP learned of on or about April 28, 2022 and first publicly acknowledged on or about July 27, 2022.

9. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, and, unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Shira Haid

10. Plaintiff Shira Haid is an adult residing in Cleveland, Wisconsin.

11. Plaintiff Haid previously received healthcare services through Common Ground Healthcare Cooperative ("Common Ground") which, upon information and belief, was a healthcare provider customer of OTP. OTP listed Common Ground Healthcare Cooperative as one of the impacted entities in its Data Breach notice.

12. To receive services from Common Ground, Plaintiff Haid was required to disclose her PII/PHI, which was then transmitted to OTP. In maintaining her PII/PHI, OTP expressly and impliedly promised to safeguard Plaintiff Haid's PII/PHI. OTP, however, did not take proper care of Plaintiff Haid's

PII/PHI, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

13. On August 3, 2022, Plaintiff Haid was locked out of her Chase Bank Mobile App while the app alerted her to possible suspicious activity. She called Chase Bank's fraud department about the suspicious activity and saw a pending wire transfer from her account for $9,500. Chase marked the transaction as fraudulent. While Plaintiff Haid was on the phone with Chase, the wire transfer went through and the funds disappeared. A second wire in the amount of $800 was fraudulently transferred from Plaintiff Haid's Chase account. In total, $10,300 was fraudulently transferred from Plaintiff Haid's account. Chase informed Plaintiff Haid that whoever fraudulently transferred the money from her account must have had her personal information to do so.

14. On August 6, 2022, Plaintiff Haid received a notice of the Data Breach from OTP. The notice stated that her personal information may have been accessed as a result of the Data Breach. She researched the company and learned that OTP was a vendor for her previous health insurer, Common Ground.

15. After discovering the fraudulent transfers, Plaintiff Haid called and visited a Chase Bank branch to fill out paperwork and attempt to retrieve her stolen money. Plaintiff Haid was left without funds in her personal checking and savings account as a result of the fraud. Plaintiff Haid's funds were later replenished by her bank. As a result of this fraud, Plaintiff Haid spent a significant amount of time addressing these issues with Chase Bank. She estimates she spent about 9 hours on the phone and in-person working to get her funds back.

16. Plaintiff Haid and Class members have faced and will continue to face a certainly impending and substantial risk of an injury as a result of OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that will continue to occur through the misuse of Class members' information.

17. Plaintiff Haid greatly values her privacy, especially as to receiving medical services. She would not have paid the amount she did to receive medical services had she known that her healthcare provider's marketing service provider would negligently fail to adequately protect her PII/PHI.

18. As a result of OTP's failure to adequately safeguard Plaintiff Haid's information, she has been injured.

Defendant OneTouchPoint Corp.

19. Defendant OneTouchPoint Corp. is a Delaware corporation with its principal place of business located at 1225 Walnut Ridge Dr., Hartland, Wisconsin 53029.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

21. This Court has personal jurisdiction over OTP because OTP maintains its principal place of business in Wisconsin.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because OTP resides in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

Overview of OTP

23. OTP is a software and business services company incorporated in Delaware with its principal place of business in Hartland, Wisconsin. OTP provides online and offline traditional marketing and communication strategies to healthcare providers. The company provides a range of services to its corporate clients, including brand management, local marketing, marketing execution, print production, and supply chain logistics.

24. In the regular course of its business, OTP collects and maintains the PII/PHI of patients, former patients, and other persons through its healthcare provider customers to whom it is currently providing or previously provided health-related or other services.

25. OTP advertises its services as allowing healthcare provider customers to serve "more patients, [with] fewer risks." It promotes the ability for a healthcare provider customer to manage its brand "across departments, clinic locations and hospital affiliates, create and execute prescriptive

marketing campaigns and enable offline and online marketing efforts at the local level – all while ensuring [a customer's] messaging and assets are compliant in this highly regulated industry."[1]

26. OTP's website tout's security as a main feature of its software, stating that its software is "designed around compliance" and it "ensure[s] compliance with state and federal regulations" and that OTP allows customers to "execute HIPAA compliant patient communications." OTP stresses that it adheres "to the strictest HIPAA standards and ensure[s] that the handling of protected health information (PHI) is secure." To this end, it "will sign a Business Associates Agreement (BAA) with [its] customers to become joint custodians of protected health information (PHI)."[2]

27. OTP further emphasizes on its website that it has "compliance expertise" and is "part of an exclusive group of organizations worldwide certified as HITRUST," explaining that its "security framework ensures that [its] solutions are built within secure web-based technology and allow[s] member communications to be published to print, web, and email." It touts the following as supporting its compliance expertise: "HIPPA compliant;" "PHI, PII, PCI, SSN, and critical system data;" "[u]ser access controls;" "[e]nd-to-end email encryption;" and "[s]ecure web interface with single sign-on."[3]

28. OTP's Privacy Policy on its website states that OTP maintains "commercially reasonable security measures to protect the Personally Identifiable Information [it] collect[s] and store[s] from loss, misuse, destruction, or unauthorized access."[4]

29. Plaintiff and Class members are or were patients whose medical records were maintained by, or who received health-related or other services from, OTP through its healthcare provider customers, and directly or indirectly entrusted OTP with their PII/PHI. Plaintiff and Class members reasonably

[1] *Healthcare*, ONETOUCHPOINT, https://1touchpoint.com/solutions/healthcare (last visited Aug. 16, 2022).
[2] *Id.*
[3] *Healthcare Insurance Member Communications*, ONETOUCHPOINT, https://1touchpoint.com/solutions/health-insurance (last visited Aug. 17, 2022).
[4] *Privacy Policy*, ONETOUCHPOINT, https://1touchpoint.com/privacy-policy (last visited Aug. 17, 2022).

expected that OTP would safeguard their highly sensitive information and keep their PII/PHI confidential.

The Data Breach

30. On or about April 28, 2022, OTP discovered encrypted files on certain computer systems. It launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity.

31. OTP's investigation determined that there was unauthorized access to certain OTP servers beginning on April 27, 2022.

32. OTP did not publicly announce the Data Breach until three months later. It provided a summary of its investigation to its healthcare provider customers beginning on June 3, 2022. It worked with its customers to determine what PII/PHI was stored on the OTP network and to whom that information related. On or around July 27, 2022, OTP began to notify patients via letter about the data breach that occurred in April 2022. The press release OTP posted on its website states: "[T]he scope of information potentially involved includes an individual's name, member ID, and information that may have provided during a health assessment."[5]

33. The company said it later determined that the compromised systems contained PII/PHI provided by its customers, including names, addresses, birth dates, date of service, description of service, diagnosis codes, information provided as part of a health assessment, and member ID. For at least one covered entity, the hacked information also contained Social Security numbers.[6]

34. OTP identified 34 healthcare insurance companies and healthcare services providers involved in the data breach, though reports indicate that number could be higher.[7]

[5] *Notice of Data Security Incident*, ONETOUCHPOINT, https://1touchpoint.com/notice-of-data-event.

[7] *See 30 Healthcare providers impacted after OneTouchPoint data breach*, SECUREBLINK (Jul. 30, 2022),https://www.secureblink.com/cyber-security-news/30-healthcare-providers-impacted-after-one-touch-point-data-breach (last visited Aug. 16, 2022) (indicating that at least two more businesses have submitted notices of being impacted by the Data Breach that were not included among those listed on OneTouch's website).

OTP Knew that Criminals Target PII/PHI

35. At all relevant times, OTP knew, or should have known, its patients', Plaintiff's, and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, OTP failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that OTP should have anticipated and guarded against.

36. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Proetus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[8]

37. PII/PHI is a valuable property right.[9] The value of PII/PHI as a commodity is measurable.[10] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[11] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[12] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

38. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites, making the information publicly available. This information from

---

[8] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Aug. 2, 2022).

[9] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[10] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[11] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[12] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

39. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[13] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[14] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[15]

40. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[16] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[17]

41. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[18] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[19]

---

[13] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[14] *Id.*

[15] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[16] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[17] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[18] *See* n.13, *supra*.

[19] *Id.*

42. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[20]

43. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

44. Theft of PII/PHI is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[21]

45. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[22] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw

[20] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[21] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Aug. 2, 2022).

[22] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[23]

46. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[24]

47. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[25]

48. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

49. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[26]

---

[23] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[24] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Aug. 2, 2022).

[25] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Aug. 2, 2022).

[26] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

50. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[27] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[28] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[29] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[30]

51. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.

[27] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.
[28] *See* n.17, *supra*.
[29] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Aug. 17, 2022).
[30] *Id.*

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[31]

52. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[32]

53. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiff and the Other Class Members

54. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) injury to their privacy; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (vii) actual fraud or attempted fraud.

CLASS ALLEGATIONS

55. Plaintiff brings this class action on behalf of herself and all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23:

> All individuals in the United States whose PII/PHI was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.

[31] *See* n.27, *supra*.
[32] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

56. Excluded from the Class is OTP and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

57. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

58. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. OTP reported that approximately 1,073,316 individuals' information was exposed in the Data Breach.

59. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether OTP had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether OTP failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

c. Whether an implied contract existed between Class members and OTP providing that OTP would implement and maintain reasonable security measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;

d. Whether OTP breached its duties to protect Plaintiff's and Class members' PII/PHI; and

e. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

60. OTP engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

61. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members

were injured by the same wrongful acts, practices, and omissions committed by OTP, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

62. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

63. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against OTP, so it would be impracticable for Class members to individually seek redress from OTP's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

64. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

65. OTP owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

66. OTP knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. OTP knew, or should have known, of the many data breaches that targeted healthcare providers in recent years.

67. Given the nature of OTP's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, OTP should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

68. OTP breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

69. It was reasonably foreseeable to OTP that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

70. But for OTP's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

71. As a result of OTP's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

72. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

73. OTP's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

74. OTP's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as OTP, of failing to employ reasonable measures to protect and secure PII/PHI.

75. OTP's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

76. OTP is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

77. OTP violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. OTP's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

78. OTP's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

79. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

80. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

81. It was reasonably foreseeable to OTP that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

82. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of OTP's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

83. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

84. Plaintiff and Class members either directly or indirectly gave OTP their PII/PHI in confidence, believing that OTP would protect that information. Plaintiff and Class members would not have provided OTP with this information had they known it would not be adequately protected. OTP's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between OTP and Plaintiff and Class members. In light of this relationship, OTP must act primarily for the benefit of its patients and health plan participants, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

85. OTP has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with

the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PII/PHI of Plaintiff and Class members it collected.

86. As a direct and proximate result of OTP's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in OTP's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT

87. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

88. Plaintiff and Class members conferred a monetary benefit upon OTP in the form of monies paid for healthcare services or other services.

89. OTP accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. OTP also benefitted from the receipt of Plaintiff's and Class members' PHI.

90. As a result of OTP's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

91. OTP should not be permitted to retain the money belonging to Plaintiff and Class members because OTP failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

92. OTP should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against OTP as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent OTP from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 17, 2022

Respectfully submitted,

/s/ Ben Barnow
Ben Barnow
b.barnow@barnowlaw.com
Anthony L. Parkhill*
aparkhill@barnowlaw.com
Riley W. Prince *
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630

Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504

Benjamin F. Johns*
bfj@chimicles.com
Samantha E. Holbrook*
seh@chimicles.com
Alex M. Kashurba*
amk@chimicles.com
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

*admission to be sought

Counsel for Plaintiff and the Proposed Class